



## UvA-DARE (Digital Academic Repository)

### The Weeping Angels are back, and they attack our privacy via smart TVs

Irion, K.; Helberger, N.

**Publication date**

2017

**Document Version**

Final published version

**License**

CC BY

[Link to publication](#)

**Citation for published version (APA):**

Irion, K. (Author), & Helberger, N. (Author). (2017). The Weeping Angels are back, and they attack our privacy via smart TVs. Web publication/site, Internet Policy Review. <https://policyreview.info/articles/news/weeping-angels-are-back-and-they-attack-our-privacy-smart-tvs/451>

**General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

## **The Weeping Angels are back, and they attack our privacy via smart TVs**

*Kristina Irion, Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands*

*Prof Dr Natali Helberger, Institute for Information Law (IViR), University of Amsterdam, Amsterdam, Netherlands*

*PUBLISHED ON: 09 Mar 2017*

One fundamental difference between traditional television sets and smart televisions is that the latter are connected to the internet. Like other connected devices, smart TVs make it possible to track what users do online and even offline, and therefore trigger privacy and data protection issues. We recently argued that the issue of media users' privacy requires special attention from policymakers, not only from the perspective of data protection law, but also from media and communication law and policy.

Tracking what people watch online can reveal sensitive insights into individual interests, political leanings, religious beliefs and cultural identity. In our article we challenge the lack of attention in media policy for the specific concerns about viewers' privacy and data protection at the EU level. The latest revelations about the CIA's attempts to turn smart TVs into eavesdropping devices (innocuously named Weeping Angel) just underscore how sensitive the issue of media users' privacy really is, and how badly it needs protection.



---

*Photo: The Weeping Angels attack – Scene from Doctor Who. Copyright: BBC.*

---

#### **SMART TV EAVESDROPPING: A WAKE UP CALL**

It is rather ironic that secret services CIA and MI5 have chosen the name of Weeping Angels from the British series Doctor Who for their joint smart TV spy program. The latest media revelations - drawing on the WikiLeaks leak *Vault 7: CIA Hacking Tools Revealed* (on 7 March 2017) - alleging that US security services are capable of using smart TVs to eavesdrop on users do not lag behind in creepiness when compared to Angels launching attacks. Of all devices, the CIA has been targeting the TV set, our trusted friend in the living room, to capture audio (even when shut down), extract the Wi-Fi network credentials the TV uses, and other usernames and passwords stored on the TV browser. This incident is yet another wake up call to European policymakers to better protect the security of connected consumer devices and the privacy and right to confidentiality of media

users.

The connective capabilities of smart TVs led to public outcries in several European countries for divulging users' privacy in a variety of ways. In 2013, the media reported that a smart TV was found to transfer information about what users are viewing to the equipment manufacturer. In 2015, the voice control of a smart TV made headlines for incidentally eavesdropping on private conversations. We reviewed a number of implementation and enforcement actions in Germany and the Netherlands. In our analysis we show how users' agency is being significantly reduced because information duties have not been complied with and how default settings were not privacy preserving. Overzealous data collection via smart TVs is not just a European issue. The US Federal Trade Commission just fined a smart TV provider for recording viewing habits of 11 million customers and selling them to third parties.

#### **BEYOND PRIVACY FREEDOM OF EXPRESSION AT STAKE**

One of the particularities of the discussion on smart TV privacy is that it is being dealt almost exclusively as an issue of data protection and privacy, and that the debate is completely oblivious to the broader and at least equally worrying implications for freedom of expression and media law and policy. In its 2013 Green Paper on Convergence, for example, the European Commission does acknowledge the fact that “the processing of personal data is often

the prerequisite for the functioning of new services, even though the individual is often not fully aware of the collection and processing of personal data”. However, the document makes it very clear that the European Commission believes that these matters should, in the first place, be a matter for EU data protection regulation. We argue, conversely, that the issue of users’ viewing privacy is also a matter for media and communication law and policy, at both the level of the EU and its member states. This is because of the potential impact that tracking users online can have on users’ freedom to inform themselves and exercise their rights to freedom of expression. Privacy in this context is instrumental in furthering our freedom of expression rights, which is why the privacy of *media users’* privacy deserves special attention. The tv set is not only the device that sees us lounging in our pyjamas on the couch (in itself reason enough to be worried about privacy). What is more important even, we use TV services to inform ourselves and prepare us for our role as informed citizens. As scholars have convincingly argued, a certain level of intellectual privacy or breathing space is indispensable for our ability to form our ideas and opinions – unmonitored by device producers, advertisers and the CIA.

The Council of Europe noted explicitly in the context of tracking users online that “[t]hese capabilities and practices can have a chilling effect on citizen participation in social, cultural

and political life and, in the longer term, could have damaging effects on democracy. ... More generally, they can endanger the exercise of freedom of expression and the right to receive and impart information protected under Article 10 of the European Convention on Human Rights”.

German data protection authorities observe that “[t]elevision is a central medium for conveying information and an essential condition for freedom of expression. The right to unobstructed information access is constitutionally protected and a basic prerequisite for the democratic order. The comprehensive collection, processing and using of information about user behaviour will adversely affect the exercise of that right”.

The Dutch data protection authority underscores that personal data collected via smart TV is sensitive because it can reveal very individual patterns which could potentially disclose the specific social background, financial or family situation. These initiatives confirm that the user of media services may require a higher, or at least different levels of protection when consuming media content than, for example, when buying shoes online. A talk by Alexander Nix of Cambridge Analytics (listen in at 9’ 22” of the video) shows just how much companies want to tap into the data of people’s viewing behaviour.

So far, only Germany has specific privacy safeguards in its media law (Section 13 and 15

Act on Telemedia). Remarkably, in Germany viewers have the right to use their TV anonymously, insofar as this is technically feasible. German law moreover prohibits the sharing of personal data on the use of television and on-demand audiovisual media services with third parties. Only anonymised usage data can be shared with third parties for market research and analytical purposes. This ties in with literature that argues in favour of protecting privacy in order to preserve the freedom to receive information and hold opinions.

#### **GET IT DONE WITH THE NEW E-PRIVACY REGULATION**

Thankfully, there are several opportunities for the European legislator to show that it has gotten the wake-up call and is moving into action to protect media users. The draft for a revised Audiovisual Media Service Directive does not mention privacy once – this should change, and the European legislator should follow the example of Germany, and introduce a right to read anonymously and protection from unauthorised data sharing at the European level.

Then, there is the new legislative proposal for a Privacy and Electronic Communications Regulation that will replace today's e-Privacy Directive. Elsewhere we explain how the Privacy and Electronic Communications Regulation could become a suitable vehicle to protect the confidentiality and security of users of interactive televisions and online content services.

The European legislator should use his exclusive competence from Article 16 of the Treaty on the Functioning of the European Union in the area of data protection to introduce provisions that protect the confidentiality and security of media consumption (and not only information in transit) against unauthorised eavesdropping from within and outside the European Union.

Remains to conclude with the note that the Angels in Doctor Who are quantum-looked creatures: they cease to move when observed – were only the intelligence agency that easy to prevent from hijacking our devices.